Einrichtung und Verfahren zur Beurteilung und Erzielung von Sicherheit bei Systemen sowie entsprechendes Computerprogramm

Stand der Technik

Die Erfindung betrifft eine Einrichtung und ein Verfahren zur Beurteilung der Sicherheit von Systemen, insbesondere im Kraftfahrzeug, in einer frühen Phase der Produktentwicklung sowie ein entsprechendes Computerprogramm bzw. Computerprogrammprodukt gemäß der Oberbegriffe der unabhängigen Ansprüche. Das Verfahren gemäß dem Oberbegriff des unabhängigen Anspruches entsprechender Kategorie wird CARTRONIC® basierte Sicherheitsanalyse (CSA) genannt und entsprechend von der Einrichtung bzw. bei Ausführung des Computerprogrammes durchgeführt.

Die Herausforderung nicht nur der Automobilindustrie ist es, steigende Anforderungen an Sicherheit und Zuverlässigkeit bei gleichzeitig verkürzten Produktentwicklungszyklen zu erfüllen. Diese Randbedingungen machen es notwendig Sicherheitsbetrachtungen bereits sehr früh während der Produktentwicklung zu berücksichtigen. Eine kurze Zeitspanne vom Beginn der Planung bis zur Markteinführung stellt einen entscheidenden Wettbewerbsvorteil dar, um ein Produkt vor den Mitbewerbern am Markt zu etablieren. Die

Berücksichtigung einer Sicherheitsanalyse in einer frühen Phase der Produktentwicklung soll langwierige Iterationen zum Testen und Verbessern des Produkts in einer fortgeschrittenen Phase der Produktentwicklung reduzieren und im Idealfall vermeiden. In einer frühen Entwicklungsphase ist die Betrachtungsweise eines Systems abstrakt, d.h. es ist bekannt welche Funktionen das System erfüllen soll und wie diese Funktionen interagieren. Es ist jedoch noch nicht festgelegt, wie diese Funktionen realisiert werden (z.B. Hardware, Software, Mechanik). Diese abstrakte Sichtweise kann durch das automobilhersteller- und zulieferneutrale Strukturierungskonzept CARTRONIC® dargestellt werden. Dieses Strukturierungskonzept bildet die Grundlage für die CARTRONIC® basierte Sicherheitsanalyse.

Die zunehmende Komplexität insbesondere des Systems Kraftfahrzeug liegt einerseits in der zunehmenden Komplexität und Anzahl der einzelnen Subsysteme, wird aber auch maßgeblich geprägt durch deren steigende Vernetzung. Die Beherrschbarkeit der Komplexität des Systems Kraftfahrzeug wird erreicht durch die Strukturierung der Subsysteme nach CARTRONIC® unter Berücksichtigung der Interaktionen mit anderen Subsystemen.

Das CARTRONIC® Strukturierungskonzept (siehe Bertram, T.; Bitzer, R.; Mayer, R.; Volkhart, A.; 1998, CARTRONIC - An open architecture for networking the control systems of an automobile, Detroit/Michigan USA, SAE 98200) basiert auf einem objektorientierten Ansatz. Das System Kraftfahrzeug wird in logische Funktionseinheiten strukturiert, die über standardisierte Schnittstellen miteinander kommunizieren.

CARTRONIC® ist ein Strukturierungskonzept für alle Steuerungs- und Regelungssysteme eines Fahrzeugs. Das Konzept enthält modulare und erweiterbare Architekturen für

„Funktion" und „Sicherheit" auf der Basis vereinbarter formaler Strukturierungs- und Modellierungsregeln.

Unter einer Architektur ist hier sowohl die Strukturierungssystematik (Regeln) zu verstehen als auch deren Umsetzung in eine konkrete Struktur. Die Funktionsarchitektur umfasst sämtliche im Fahrzeug vorkommenden Steuerungs- und Regelungsaufgaben. Die Aufgaben des Systemverbunds werden sog. funktionalen Komponenten zugeordnet, die Schnittstellen der Komponenten (funktionale Schnittstellen) und ihr Zusammenwirken werden festgelegt. Die Sicherheitsarchitektur erweitert die Funktionsarchitektur um Elemente, die einen sicheren Betrieb des Systemverbunds garantieren.

Eine weitere Darstellungsform ergibt sich durch Abblidung in UML (Unified Modelling Language), was außerdem eine Portierung auf ein Computersystem erleichtert. Die Abbildung einer CARTRONIC®-Funktionsstruktur in ein UML-Modell ist beschrieben in (Torre Flores, P.; Lapp, A.; Hermsen, W.; Schirmer, J.; Walther, M.; Bertram, T.; Petersen, J.; 2001, Integration of a structuring concept for vehicle control systems into the software development process using UML modeling methods, Detroit/Michigan USA, SAE 2001-01-0066).

Das Grundgerüst für die Strukturierung bildet die funktionale Komponente. Eine funktionale Komponente repräsentiert eine Funktion im System Kraftfahrzeug. Zu Gunsten einer kompakten Darstellung wird im folgenden anstelle des Begriffs funktionale Komponente lediglich der Begriff Komponente verwendet. Die Komponenten können im Laufe der Entwicklung verfeinert (detailliert) werden, wobei die übergeordnete Funktion als Hülle erhalten bleibt. Die übergeordnete Funktion wird innerhalb der Verfeinerung (Detaillierung) wiederum aus Komponenten zusammengesetzt, die einzelne Teile der übergeordneten Funktion

repräsentieren. Bei dem Strukturierungskonzept werden drei verschiedene Typen von Komponenten unterschieden:

- Komponenten mit überwiegend koordinierenden und verteilenden Aufgaben,
- Komponenten mit hauptsächlich operativen und ausführenden Aufgaben und
- Komponenten, die ausschließlich Informationen generieren und bereitstellen.

Bei den Kommunikationsbeziehungen wird zwischen einem Auftrag (mit Rückmeldung), einer Abfrage (mit Hinweis) und einer Anforderung unterschieden. Den Auftrag kennzeichnet die Pflicht zur Ausführung; für den Fall der Nichterfüllung muss der Auftragnehmer eine Rückmeldung an den Auftraggeber absetzen, die den Grund für die Nichtausführung beschreibt. Die Abfrage dient der Beschaffung von Informationen für eine Auftragsausführung. Für den Fall, dass eine Komponente die abgefragte Information nicht bereitstellen kann, gibt sie einen Hinweis an die fragende Komponente. Eine Anforderung beschreibt einen „Wunsch" , dass eine Funktion von einer anderen Komponente ausgeführt wird. An die Anforderung ist allerdings nicht die Pflicht zur Erfüllung gekoppelt, was beispielsweise bei konkurrierenden Anforderungen Berücksichtigung findet. Tabelle 1 stellt die Strukturelemente zusammenfassend dar.

Tabelle 1

STRUKTURELEMENT	KURZBESCHREIBUNG
Funktionale Komponente (kurz: Komponente)	Funktionseinheit mit klar definierter Aufgabe
System	Ein System besteht aus mehreren funktionalen Komponenten bzw. (Sub-) Systemen. („Sicht von innen nach außen"). Die detaillierte funktionale Komponente leitet die Kommunikationsbeziehungen an die

	Teilkomponenten weiter, wie dies eine „ist Teil von" -Beziehung ausdrückt. („Sicht von außen nach innen)
Auftrag (mit Rückmeldung)	Handlungsanweisung an eine funktionale Komponente mit der Pflicht zur Ausführung.
Abfrage (mit Hinweis)	Informationsabfrage an eine funktionale Komponente.
Anforderung	Anforderung an eine funktionale Komponente ohne Ausführungsverpflichtung
Regeln	Regeln zu: ❑ Kommunikationsbeziehungen ❑ Modellierungsmustern

Die Strukturierungsregeln beschreiben erlaubte Kommunikationsbeziehungen innerhalb der Architektur des Gesamtfahrzeugs. Es werden Strukturierungsregeln unterschieden, welche die Kommunikationsbeziehungen auf der gleichen Abstraktionsebene und in höhere und tiefere Ebenen unter Berücksichtigung angegebener Randbedingungen festlegen. Ferner klären die Strukturierungsregeln die Weiterleitung von Kommunikationsbeziehungen hinein in die Detaillierung einer anderen Funktionalität.

Eine nach den Strukturierungs- und Modellierungsregeln entwickelte Struktur zeichnet sich durch folgende Merkmale aus:

- ❑ vereinbarte, einheitliche Strukturierungs- und Modellierungsregeln auf allen Abstraktionsebenen,
- ❑ hierarchische Auftragsflüsse,
- ❑ hohe Eigenverantwortung der einzelnen Komponenten,
- ❑ Bedienelemente, Sensoren und Schätzer sind gleichwertige Informationsgeber und eine
- ❑ Kapselung, die jede Komponente für die übrigen Komponenten so sichtbar wie nötig und so unsichtbar wie möglich darstellt.

Es stellt sich somit die Aufgabe ein Verfahren und eine Einrichtung sowie ein entsprechendes Computerprogramm und Computerprogrammprodukt zu generieren, welches eine verbesserte Sicherheitsanalyse und Erzeugung einer verbesserten Sicherheitsstruktur wenigstens eines Systems, insbesondere in einem Kraftfahrzeug ermöglicht.

Vorteile der Erfindung

Die Erfindung betrifft eine Einrichtung, insbesondere ein Computersystem, und ein Computerprogramm oder Computerprogrammprodukt, sowie ein Verfahren zur Durchführung einer Sicherheitsanalyse bei Systemen, insbesondere in einem Kraftfahrzeug, wobei die Systeme oder das wenigstens eine System aus mehreren Komponenten bestehen, zwischen denen Kommunikationsbeziehungen bestehen, wobei die Komponenten und deren Kommunikationsbeziehungen eine Funktionsstruktur der Systeme oder des wenigstens einen Systems bilden, wobei vorteilhafter Weise Fehler in Abhängigkeit von der Funktionsstruktur ermittelt werden und diese Fehlerabhängigkeiten bezüglich der Funktionsstruktur ausgewertet werden.

In einer Ausführungsform zeigt die Erfindung eine Einrichtung, insbesondere ein Computersystem, und ein Computerprogramm oder Computerprogrammprodukt sowie ein Verfahren zur Erzielung einer vorgebbaren Sicherheitsstufe bei Systemen, insbesondere in einem Kraftfahrzeug, wobei die Systeme oder wenigstens ein System aus mehreren Komponenten bestehen, zwischen denen Kommunikationsbeziehungen bestehen, wobei die Komponenten und deren Kommunikationsbeziehungen eine Funktionsstruktur der Systeme bilden, wobei Fehler in Abhängigkeit von der Funktionsstruktur ermittelt werden und diese

Fehlerabhängigkeiten bezüglich der Funktionsstruktur ausgewertet werden mit folgenden Schritten:

a) Verfolgung der Fehlerabhängigkeiten in der Funktionsstruktur und Generierung von Fehlerpfaden sowie Ermittlung von globalen Auswirkungen der Fehler,
b) Bewertung der globalen Auswirkungen in Abhängigkeit vorgebbarer Sicherheitsstufen,
c) Ermittlung von Fehlern, welche ein Fehlverhalten einer Komponente oder einer Kommunikationsbeziehung bewirken,
d) Zuordnung des Fehlverhaltens einer Komponente oder einer Kommunikationsbeziehung zu den globalen Auswirkungen
e) Ermittlung von Maßnahmen zur Fehlererkennung und/oder Fehlerbeherrschung,
f) Ermittlung der erzielbaren Sicherheitsstufe und Vergleich der ermittelten Sicherheitsstufe mit der zu erzielenden Sicherheitsstufe und
g) in Abhängigkeit von dem Vergleich erneuter Verfahrensstart bei a), bis die zu erzielende Sicherheitsstufe erzielt ist.

Vorteilhafter Weise erfolgt damit die Durchführung einer Sicherheitsanalyse in einer frühen Phase der Produktentwicklung, um Problembereiche rechtzeitig zu erkennen und die frühzeitige Integration von Sicherheitsmaßnahmen in die Funktionsstruktur („safety through design").

Die erfindungsgemäße Sicherheitsanalyse ist somit zweckmäßiger Weise auch als ein iterativer Analyse- und Verbesserungsprozess dargestellt.

Das Verfahren zur Beurteilung der Sicherheit von Systemen kann vorteilhafter Weise auf Basis von CARTRONIC®-Funktionsstrukturen bzw. von CARTRONIC®-UML-Modellen dargestellt werden, lässt sich aber auch auf andere Systemmodellierungen übertragen.

Das Verfahren wird zweckmäßiger Weise mittels der CSA-Tabelle durchgeführt. Durch die CSA-Tabelle werden globale Fehlerauswirkungen identifiziert und bewertet. Sie dokumentiert Fehlerabhängigkeiten von Komponenten und Kommunikationsbeziehungen. Ein Fehlverhalten wird dabei verursacht durch Funktionsstruktur-Fehler (FS-Fehler) in Komponenten oder Kommunikationen. Kommunikationsfehler (Aufträge, Anforderungen) werden bei der Zielkomponente der Kommunikation berücksichtigt. FS-Fehler bei Abfragen werden bei der Quellkomponente der Kommunikation berücksichtigt.

Ein Fehlverhalten der Komponenten wird den globalen Auswirkung zugeordnet. Dadurch erreicht man nicht nur eine Beurteilung globaler Zustände, sondern auch welche Komponenten der Funktionsstruktur dafür verantwortlich sind.

Das Verfahren ist in einer speziellen Ausführungsform in einen CARTRONIC® basierten Entwicklungsprozess integriert. Dadurch wird ein formales, systematisches Vorgehen gefördert.

Die Sicherheitsmaßnahmen werden insbesondere in ein CARTRONIC®-UML-Modell abgebildet. Dies ermöglicht eine formale Verifikation gegenüber festgelegten Produktanforderungen oder der Produktspezifiktion. Eine Validierung der Produktspezifikation ist bei dieser Vorgehensweise auch möglich.

Somit kann vorteilhaft die Durchführung weiterführender quantitativer Sicherheitsbetrachtungen auf Grundlage der CSA-Tabelle, der CARTRONIC®-Funktionsstruktur oder des CARTRONIC®-UML-Modells inklusive Sicherheitsmaßnahmen erzielt werden.

Weitere Vorteile und vorteilhafte Ausgestaltungen ergeben sich aus der Beschreibung und/oder den Merkmalen der Ansprüche.

Zeichnung

Die Erfindung wird nachfolgend anhand der durch die Figuren dargestellten Zeichnungen und Tabellen näher erläutert.

Dabei zeigt Figur 1 das Verfahren bzw. die Vorgehensweise bei der Sicherheitsanlayse.

Figur 2 zeigt die CARTRONIC®-Funktionsstruktur eines beispielhaft betrachteten Bremssystems.

Figur 3 stellt ein Beispiel für eine UML-Modellierung der CARTRONIC®-Funktionsstruktur nach Figur 2 dar.

Figur 4 zeigt den Tabellenkopf der CSA-Tabelle mit den globalen Auswirkungen dar.

Figur 5 zeigt die Zuordnung der Fehlerauswirkungen zu den Sicherheitsstufen in einem Flußgraphen.

Figur 6 zeigt beispielhaft eine Bewertung der globalen Auswirkungen.

Figur 7 zeigt die Fehlerfortpflanzung in der Funktionsstruktur bzw. die Zuordnung von FS-Fehlern zu den globalen Auswirkungen.

Figur 8 bestehend aus den Einzelfiguren 8a, 8b, 8c und 8d zeigt die CSA-Tabelle, also die Sicherheitstabelle, gemäß dem Beispiel nach Figur 2 mit den entsprechenden Kennzeichen.

Figur 9 zeigt die Einordnung der CSA in einen Entwicklungsprozess, insbesondere nach V-Modell

Beschreibung der Ausführungsbeispiele

Die im folgenden beschriebene Sicherheitsanalyse beruht auf der CARTRONIC®-Funktionsstruktur bzw. dem CARTRONIC®-UML-Modell des betrachteten Systems. Das CARTRONIC®-UML-Modell ist die Abbildung einer CARTRONIC®-Funktionsstruktur in die UML (Unified modeling language). Durch die Abbildung in die UML erhält man eine formalisierte und genauer spezifizierte Darstellung, welche eine automatisierte Realisierung der Erfindung erleichtert. Die Abbildung einer CARTRONIC®-Funktionsstruktur in ein UML-Modell ist beschrieben in (Torre Flores, P.; Lapp, A.; Hermsen, W.; Schirmer, J.; Walther, M.; Bertram, T.; Petersen, J.; 2001, Integration of a structuring concept for vehicle control systems into the software development process using UML modeling methods, Detroit/Michigan USA, SAE 2001-01-0066).

Die CARTRONIC® basierte Sicherheitsanalyse ist ein Verfahren zur systematischen Sicherheitsanalyse auf abstrakter Systemebene und unterstützt somit das Entwicklungskredo „safety through design" . Die in einer früheren Veröffentlichung beschriebene Vorgehensweise zur CARTRONIC® basierten Sicherheitsanalyse (Bertram, T.; Dominke, P.; Müller, B., 1999, The Safety-Related Aspect of CARTRONIC, Detroit/Michigan USA, SAE'99, Session Code PC 26) wird grundlegend überarbeitet und erweitert um die Analyse struktureller Fehlerabhängigkeiten. Durch die Verwendung des Verfahrens in einer frühen Entwicklungsphase können Fehler

und deren Ursachen abstrakt beschrieben werden, z.B. „Fehler vorhanden" oder „Fehler nicht vorhanden" . Das Verfahren stellt somit eine Abstraktion der FMEA (Failure Mode and Effects Analysis oder Fehler-Möglichkeits- und Einfluß-Analyse) dar, welches erweitert ist um die Analyse struktureller Fehlerabhängigkeiten. Die FMEA ist dabei ein anerkanntes methodisches Verfahren zur Analyse, Bewertung und Dokumentation von Systemen, Bauteilen und Herstellungsprozessen und dient vornehmlich der Fehlervermeidung. Die Intention der CSA ist nicht eine FMEA zu ersetzen, sondern lediglich in einer frühen Entwicklungsphase die Systementwickler bei der Identifikation von potentiellen Gefahrenstellen zu unterstützen.

Zunächst werden wichtige Begriffe definiert, bevor die Erfindung dann anhand eines Beispiels erläutert wird.

Definition 1 (globale Auswirkungen)
Globale Auswirkungen sind physikalische Effekte, die sich durch Aktuatoren auf das Gesamtsystem Kraftfahrzeug auswirken. Sie werden von Sensorik (oder auch einem Fahrzeugführer) bemerkt durch Funktionsverlust (z.B. Versagen des Bremssystems) oder Komforteinbuße (z.B. durch Abschaltung von Assistenzsystemen wie beispielsweise Adaptive Cruise Control).

Definition 2 (Funktionsstruktur-Fehler)
Funktionsstruktur-Fehler (FS-Fehler) sind Fehler, die ein Fehlverhalten einer Komponente oder einer Kommunikation bewirken.

Definition 3 (Funktionsstruktur-Fehler-Ursachen)
Funktionsstruktur-Fehler-Ursachen (FS-Fehler-Ursachen) sind Gründe für ein Fehlverhalten einer Komponente. Der Grund für ein Fehlverhalten einer Komponente liegt im Vorhandensein von FS-Fehlern. FS-Fehler können weiter unterteilt werden in verfeinerte Fehlerarten. Die verfeinerten Fehlerarten sind

dann wiederum die Ursache für die FS-Fehler. Die verfeinerten Fehlerarten können sein:

Komponentenfehler:
Komponente tot
Komponente berechnet falsche Werte
Komponente ist unkontrolliert aktiv
Komponente generiert Ergebnis zur falschen Zeit

Kommunikationsfehler:
Kommunikation unterbrochen
Kommunikation liefert falsche Information
Kommunikation ist unkontrolliert aktiv
Kommunikation liefert Information zur falschen Zeit
Kommunikation ist fehlgeleitet

Figur 1 zeigt die Vorgehensweise der CARTRONIC® basierten Sicherheitsanalyse. Das Verfahren kann folgendermaßen gegliedert werden:

Schritt 1: Globale Auswirkungen identifizieren auf Basis der CARTRONIC®-Funktionsstruktur bzw. des CARTRONIC®-UML-Modells

Schritt 2: Globale Auswirkungen bewerten durch Sicherheitsstufen (SL)

Schritt 3: Analyse von FS-Fehler-Ursachen (vgl. *Definition 3*), d.h. Fehler von Komponenten oder Kommunikationsbeziehungen analysieren

Schritt 4: Zuordnung eines Fehlverhaltens einer Komponente zu den globalen Auswirkungen

Schritt 5: Maßnahmen zur Fehlererkennung und/oder Beherrschung ermitteln

Schritt 6: Erstellung bzw. Ergänzung einer CARTRONIC®-Sicherheitsstruktur

Schritt 7: Verifikation der resultieren Funktions- und Sicherheitsstruktur unter Sicherheitsaspekten

Im folgenden wird die Vorgehensweise der CARTRONIC® basierten Sicherheitsanalyse anhand eines Beispiels beschriebenen. Als Beispiel wurde ein vereinfachtes Bremssystem gewählt. Die CARTRONIC®-Funktionsstruktur und das CARTRONIC®-UML Modell des vereinfachten Bremssystems ist in Figur 2 und Figur 3 dargestellt. Das Beispielsystem besteht aus den Komponenten *Momentenverteiler*, *Vortrieb*, *Bremssystem*, *Bremssystemkoordinator*, *Bremsaktuator* und *Bremslicht*. In der logischen, hierarchischen Funktionsstruktur von CARTRONIC® befinden sich die Komponenten *Bremssystemkoordinator* und *Bremsaktuator* in der Detaillierung des Bremssystems. Die Komponenten *Momentenverteiler*, *Vortrieb* und *Bremssystem* sind Detaillierungen von *Vortrieb und Bremse*. In der Funktionsstruktur ist *Vortrieb und Bremse* eine Detaillierung der *Fahrzeugbewegung*. Die Komponente *Bremslicht* befindet sich in der Detaillierung von *Licht und Lichtzeichen*, das eine Detaillierung von *Außenbeleuchtung* ist. *Diese ist wiederum eine Verfeinerung der Komponente Sichtbarkeit und Signalisierung* in *Karosserie und Innenraum*. Die Detaillierungen von *Fahrzeugbewegung* und *Karosserie und Innenraum* sind in der *Fahrzeugebene* platziert. Die *Fahrzeugebene* ist die oberste Ebene der CARTRONIC®-Funktionsstruktur. Der *Momentenverteiler* ist dafür zuständig die Momentenwünsche des Fahrzeugführers zu verteilen. Die Komponenten *Bremssystemkoordinator* und *Vortrieb* fordern Momente beim *Momentenverteiler* über die Kommunikationen R1 und R2 an. Liegt nur eine Anforderung vom *Vortrieb* vor, so fragt der *Momentenverteiler* minimal und maximal zulässige Momentenwerte von der Komponente *Vortrieb* durch die Kommunikation I1 ab und sorgt dann für die Umsetzung durch den Auftrag O2. Liegt nur eine Anforderung vom *Bremssystem* vor, dann wird diese durch den Auftrag O1 realisiert. Liegen Anforderungen von *Vortrieb* und *Bremssystem vor*, so hat das *Bremssystem* vorrang. Die Komponente *Bremssystemkoordinator* in der Detaillierung des *Bremssystems* sorgt durch den Auftrag O3 an den *Bremsaktuator* für die Umsetzung der Momente und mit der Anforderung R3 für die

Ansteuerung des *Bremslichts*, damit wird der Fahrerwunsch nachfolgenden Fahrzeugen signalisiert.

Die Erkenntnisse der CARTRONIC® basierten Sicherheitsanalyse werden in Form einer Tabelle, der CSA-Tabelle, übersichtlicht zusammengefasst und gespeichert.

Durch die CSA-Tabelle erreicht man eine Zuordnung von einem Fehlverhalten einer einzelnen Komponente zu Fehlerabhängigkeiten innerhalb der Funktionsstruktur. Die in der CSA-Tabelle dokumentierten FS-Fehler können zu den oben angegebenen Fehlerarten verfeinert werden. Die verfeinerten Fehlerarten sind auf abstrakter Systemebene interpretierbar als Ursache für die FS-Fehler. Des weiteren werden die „internen Auswirkungen" (Fehlverhalten einer Komponente) den globalen Auswirkungen zugeordnet. Hierdurch werden komplexe Abhängigkeiten zwischen strukturinternen Fehlerabhängigkeiten und globalen Auswirkungen erkennbar.

Das im folgenden beschriebene Verfahren stellt bzgl. der Ursachenanalyse einen „bottom-up" -Ansatz dar, da ausgehend von einem potentiellen Fehlverhalten die möglichen Ursachen dafür identifiziert werden. Die Vorgehensweise wird nun anhand des oben erläuterten Beispiels und der bereits dargestellten Schritte 1-7 erklärt:

Schritt 1: Globale Auswirkungen identifizieren

Globale Auswirkungen ergeben sich bei Betrachtung der Systemschnittstelle zur Umgebung. Die Aktuatoren, welche von dem betrachteten Subsystem angesteuert werden, repräsentieren die Schnittstellen zur Umgebung. In dem hier betrachteten Kontext bedeutet Umgebung das Kraftfahrzeug als Ganzes. Die Aktuatoren für das in Figur 2 und Figur 3 dargestellte Beispielsystem sind das *Bremssystem* bzw. in der Detaillierung der *Bremsaktuator*, der

Vortrieb und das *Bremslicht*. Es werden lediglich solche globalen Auswirkung betrachtet und z.B. in einem Computersystem erfaßt, die von dem zu untersuchenden Subsystem zu verantworten sind. So ist es z.B. nicht sinnvoll das Adaptive Cruise Control (ACC) Subsystem, welches das Bremssystem ansteuert, für einen Totalverlust der Bremswirkung verantwortlich zu machen. Diese Zusammenhänge sind mittels Zuordnungstabellen oder Expertensystemen erfassbar und werden im Verfahrensverlauf durch das Computersystem zugreifbar zur Verfügung gestellt. Bei iterativem Vorgehen können dann je nach Iterationsvorgang unterschiedliche Zusammenhänge in oben dargestellter Form Anwendung finden. Dies gilt auch für das weitere Vorgehen wie nachfolgend beschrieben.

Für das in Figur 2 dargestellte Beispiel können beispielsweise die nachfolgenden globalen Auswirkungen identifiziert werden:

- ❑ Beschleunigungswirkung → Vortrieb
  - Unkontrollierte Beschleunigung
    - o Beschleunigung zu stark
    - o Beschleunigung zu schwach
  - Keine Beschleunigung
- ❑ Bremswirkung → Bremsaktuator
  - Keine Bremswirkung
  - Zu geringe Bremswirkung
- ❑ Signalisierung → Bremslicht
  - Keine Anzeige
  - Kontinuierliche Anzeige (enthält Szenario Bremslicht leuchtet, obwohl nicht gebremst wird)

In Figur 4 ist der Tabellenkopf mit den globalen Auswirkungen der CSA-Tabelle dargestellt.

Schritt 2: Globale Auswirkungen bewerten durch Sicherheitsstufen

Die Bewertung der globalen Auswirkungen erfolgt in Anlehnung an die Anforderungsklassen, die in der DIN V 19250 definiert sind. Die Anforderungsklassen in der Norm sind allgemein für MSR-Schutzeinrichtungen (MSR - Messen, Steuern, Regeln) definiert. Die Voraussetzungen, die dort festgelegt sind, lassen sich nicht direkt auf Kraftfahrzeuge übertragen. In dieser Norm fließen die Punkte

- Aufenthaltsdauer im Gefahrenbereich
- eine oder mehrere Personen sind von den potentiellen Auswirkungen eines Fehlers betroffen

in die Bewertung ein. Bei Kraftfahrzeugen ist die Berücksichtigung dieser Fälle hingegen nicht sinnvoll. Sie sind unter der Prämisse zu betrachten, dass beim Betrieb bestimmter Maschinen eine Person, welche die Maschine bedient, diese von einem Prüfstand aus betätigt und nur unter bestimmten Voraussetzungen für eine begrenzte Zeitdauer, z.B. bei Wartungsarbeiten, einer potentiellen Gefahr ausgesetzt ist. Im Kraftfahrzeug ist man hingegen ständig einer potentiellen Gefahr ausgesetzt. Außerdem können immer mehrere Personen von den Auswirkungen eines Fehlers betroffen sein. Bei Beachtung dieser Einwendungen kommt man zu angepassten „Anforderungsklassen" für Automobile, die im Rahmen der CSA als Sicherheitsstufen (engl. safety level - SL) bezeichnet werden. Die Zuordnung der Sicherheitsstufen zu Fehlerauswirkungen ist in dem Risikograph von Figur 5 dargestellt.

Es wird unterschieden, ob eine Auswirkung im Einzelfall oder im Regelfall auftritt. Im Einzelfall bedeutet, dass in der überwiegenden Mehrheit der Fälle nicht mit der entsprechenden Auswirkung gerechnet werden muss. Den Sicherheitsstufen können Ereignishäufigkeiten zugeordnet werden. Eine solche Ereignishäufigkeit ist als Sollgröße zu verstehen, die von der späteren Realisierung einer Komponente mindestens zu erfüllen ist. Eine a priori Verifikation der Ereignishäufigkeiten ist in der Regel nicht möglich, da verlässliche Daten oft erst nach einem Serieneinsatz zur Verfügung stehen. Es ist jedoch möglich

den mit einer Sicherheitsstufe verbundenen Sollwert der Ereignishäufigkeit nachträglich mit einem erfassten Istwert zu vergleichen. Tritt hierbei eine Abweichung auf, d.h. ist die tatsächlich ermittelte Ereignishäufigkeit größer, als die zulässige Ereignishäufigkeit einer Sicherheitsstufe, so müssen Maßnahmen zur Reduktion der Ereignishäufigkeit getroffen werden.

In Figur 6 ist die Bewertung der globalen Auswirkungen des Bremssystems durch Sicherheitsstufen abgebildet. Ein Bremssystem ist eine äußerst wichtige Funktionalität eines Kraftfahrzeugs, die unter allen Umständen gewährleistet sein muss. Die globale Auswirkung „keine Bremswirkung" stellt im Regelfall eine Bedrohung für Leib und Leben dar, die vom Fahrzeugführer nicht beherrschbar ist. Deshalb muss hier die Sicherheitsstufe SL4 vergeben werden. Für die Auswirkung „keine Beschleunigung" wird die Sicherheitsstufe SL1 vergeben, weil hier im Regelfall davon ausgegangen werden kann, dass mit maximal leichten Verletzungen zu rechnen ist, z.B. durch Auffahrunfälle mit geringer Geschwindigkeitsdifferenz. In Einzelfällen kann eine Gefahr für Leib und Leben bestehen, die jedoch beherrschbar ist, z.B. einschalten der Warnblinkanlage.

Um im folgenden eine übersichtliche Darstellung zu erhalten wird auf die Verfeinerung der Tabellenspalte „Unkontrollierte Beschleunigung" verzichtet.

Schritt 3: Funktionsstruktur-Fehler-Ursachenanalyse

Bei der Ursachenanalyse wird die Frage gestellt: Was verursacht ein Fehlverhalten einer Komponente {Momentenverteiler, Vortrieb, Bremssystem, Bremssystemkoordinator, Bremsaktuator, Bremslicht}?

Die Ursachenanalyse untersucht, wodurch ein Fehlverhalten der CARTRONIC®-Komponenten {Momentenverteiler, Vortrieb, Bremssystem, Bremssystemkoordinator, Bremsaktuator, Bremslicht} bedingt sein könnte. Untersucht wird ein Fehlverhalten von

Komponenten und ihren Detaillierungen, soweit diese bekannt sind. Zur Ursachenanalyse wird die CARTRONIC®-Funktionsstruktur des betrachteten Systems in die Kopf**zeile** „Funktionsstruktur" der CSA-Tabelle übernommen. Außerdem wird die CARTRONIC®-Funktionsstruktur in die **Spalte** „Fehlverhalten Komponenten" übernommen. (siehe Figur 7).

Falls ein FS-Fehler in einer Komponente ein Fehlverhalten in der selben Komponente verursacht erfolgt die Zuordnung der Komponente aus der Funktionsstruktur zu einem Fehlverhalten der selben Komponente (Kennzeichnung mit „x" , vgl. Figur 7). Zusätzlich werden auch für die Komponente relevante FS-Fehler der Kommunikationsbeziehungen berücksichtigt. Verursacht ein FS-Fehler einer Kommunikationsbeziehung ein Fehlverhalten, so erfolgt ebenfalls eine Zuordnung zur Funktionsstruktur, welche die Art und den Namen der betrachteten Kommunikation wiedergibt. Die Art der Kommunikationsbeziehung wird mit dem großgeschriebenen Anfangsbuchstaben des englischen Ausdrucks der Kommunikation bezeichnet. Folglich wird für einen Auftrag (engl. Order) ein „O" , für eine Anforderung (engl. Request) ein „R" und für eine Abfrage (engl. Inquiry) ein „I" verwendet. Der Art der Kommunikation folgt ein Unterstrich „_" , dem sich der Name der Kommunikationsbeziehung anschließt (z.B. I_I1).

Bei der Ursachenanalyse für ein Fehlverhalten einer Komponente wird die

- **Komponente** selbst, sowie
- ankommende **Aufträge**
- ankommende **Anforderungen**
- abgehende **Abfragen**

betrachtet.

Im weiteren Verlauf werden die Fehlerabhängigkeiten untersucht. Es wird somit ermittelt, welche weiteren Komponenten und Kommunikationen für ein Fehlverhalten der betrachteten Komponente verantwortlich sein können. Hierfür werden die in der Spalte M einer Komponente stehende(n) Kommunikation(en)

zurückverfolgt und die neu gefundene(n) Komponente(n) in der selben Zeile dem Komponentenfehlverhalten zugeordnet. Eine der neu gefundenen Komponenten dient als neuer Ausgangspunkt. Die dieser Komponente zugeordnete(n) Kommunikation(en) werden ermittelt und in der Spalte M der entsprechenden Komponente aufgenommen. Es werden wiederum die dieser Komponente zugeordneten Kommunikationen zurückverfolgt. Damit werden neue Ausgangskomponenten gefunden. Dieser Vorgang wird so lange iterativ fortgeführt, bis keine weiteren Kommunikationen vorhanden sind bzw. alle erreichbaren Komponenten durchlaufen wurden (vgl. nachfolgendes Beispiel und Figur 8).

Beispiel:

Ein Fehlverhalten der Komponente *Momentenverteiler* (fc_1) hat die Ursache darin, dass ein Komponentenfehler in der Komponente *Momentenverteiler* (fc_1) selbst, ein Kommunikationsfehler in der *Abfrage I1* oder der *Anforderung R1* oder der *Anforderung R2*, ein Komponentenfehler in der Komponente *Vortrieb* (fc_3) oder ein Kommunikationsfehler im *Auftrag O2* bzw. ein Komponentenfehler in der Komponente *Bremssystemkoordinator* (fc_{21}) oder im *Auftrag O1* aufgetreten ist.

Ein Fehlverhalten der Komponente *Bremssystem* (fc_2) hat die Ursache darin, dass entweder ein Komponentenfehler in dem *Bremssystem* (fc_2) selbst vorliegt oder ein Kommunikationsfehler im *Auftrag O1* oder ein Komponentenfehler im *Momentenverteiler* (fc_1) mit den hier zu berücksichtigenden potentiellen Kommunikationsfehlern *Anforderung R1*, *Anforderung R2* und *Abfrage I1* oder ein Fehler in der Komponente *Vortrieb* (fc_3) oder ein Kommunikationsfehler im *Auftrag O2* aufgetreten ist.

Die Einträge in der CSA-Tabelle für das in Figur 2 dargestellte Beispiel, sind aus Figur 8, insbesondere Figur 8a, ersichtlich.

Wird ein Fehlverhalten einer Komponente in der Verfeinerung betrachtet, so ist die Hülle für die Ursachenanalyse nicht von

Interesse, da nur Kommunikationsbeziehungen von der höheren Ebene in die Verfeinerung weitergeleitet werden. Die Spalte *Bremssystem* (*Bremssystem* (fc_2) ist Hülle von *Bremssystemkoordinator* und *Bremsaktuator*) der „Funktionsstruktur" muss für die Ursachenanalyse eines Fehlverhaltens der Komponente *Bremssystemkoordinator* (Zeile *Bremssystemkoordinator* (fc_{21}) in der Spalte „Fehlverhalten Komponenten") nicht berücksichtigt werden. Bei der Ursachenanalyse eines Fehlverhaltens der Komponente *Bremslicht* ist es nicht notwendig die Analyse für die Komponente *Bremssystem* durchzuführen, falls die Analyse für die Verfeinerung der Komponente *Bremssystem* durchgeführt wurde. Mögliche Ursachen werden bei der Betrachtung der Verfeinerung (*Bremssystemkoordinator* und *Bremsaktuator*) bereits berücksichtigt.

Die CSA Tabelle erlaubt somit eine Verfolgung von logischen Fehlerabhängigkeiten. Die Spalten der Funktionsstruktur mit vielen Einträgen z.B. Spalte *Momentenverteiler* (fc_1) und Spalte *Vortrieb* (fc_3) sind wichtige Komponenten, da sich dort ein Fehler auf große Teile des Systems auswirkt.

Schritt 4: Zuordnung eines Fehlverhaltens einer Komponente zu den globalen Auswirkungen

Zunächst werden also die in Schritt 1 identifizierten globalen Auswirken den Komponenten zugeordnet, deren Fehlverhalten eine globale Auswirkung verursacht. Diese Komponenten sind die System-Schnittstellen (siehe Schritt 1).

Unter Schritt 1 ist diese Zuordnung bereits dargestellt.

- ❑ Beschleunigungswirkung → Fehlverhalten Vortrieb
- ❑ Bremswirkung → Fehlverhalten Bremsaktuator
- ❑ Signalisierung → Fehlverhalten Bremslicht

Diese Zuordnung in der CSA-Tabelle ist aus Figur 8b ersichtlich.

Durch die Fehlerabhängigkeiten, die in Schritt 3 ermittelt wurden, erhält man eine Zuordnung der übrigen Komponenten zu den globalen Auswirkungen. Dies erreicht man durch Betrachtung der Spalten der Funktionsstruktur für die Zeilen der System-Schnittstellen (Fehlverhalten der Komponenten *Bremsaktuator* (fc_{22}), *Vortrieb* (fc_3) und *Bremslicht* (fc_4)). Jede Spalte der Funktionsstruktur, die einem Fehlverhalten der System-Schnittstellen zugeordnet ist, d.h. mit einem „x" gekennzeichnet ist, kann die selben globalen Auswirkungen verursachen. Der Hülle einer Detaillierung werden alle globalen Auswirkungen zugeteilt, die den Komponenten der Detaillierung zugeordnet sind. Das Resultat dieses Schrittes ist in Figur 8c dargestellt.

Beispiel:

Im folgenden wird die Komponente *Momentenverteiler* (fc_1) in der Funktionsstruktur betrachtet. Die Komponente *Momentenverteiler* (fc_1) in der Funktionsstruktur ist der Zeile Fehlverhalten *Bremsaktuator* (fc_{22}) zugeordnet, d.h. ein FS-Fehler in der Komponente *Momentenverteiler* kann ein Fehlverhalten des *Bremsaktuators* verursachen. Daraus kann gefolgert werden, dass ein Fehlverhalten der Komponente *Momentenverteiler* auch die globalen Auswirkungen des *Bremsaktuators* verursachen kann. Die globalen Auswirkungen eines Fehlverhaltens des *Bremsaktuators* („keine Bremswirkung" und „zu geringe Bremswirkung") werden somit auch dem Fehlverhalten des *Momentenverteilers* zugeordnet. Außerdem kann ein FS-Fehler in der Komponente *Momentenverteiler* (fc_1) ein Fehlverhalten des *Vortriebs* (fc_3) verursachen. Ein Fehlverhalten der Komponente *Momentenverteiler* kann somit auch die globalen Auswirkungen „unkontrollierte Beschleunigung" und „keine Beschleunigung" bewirken. Ein FS-Fehler in der Komponente *Momentenverteiler* (fc_1) kann ein Fehlverhalten des *Bremslichts* (fc_4) verursachen. Somit kann ein Fehlverhalten der Komponente *Momentenverteiler* die globalen Auswirkungen „keine Anzeige" und „kontinuierliche Anzeige" verursachen.

Ein Fehlverhalten des *Bremssystems* (fc_2) als Hülle der Komponenten *Bremssystemkoordinator* (fc_{21}) und *Bremsaktuator* (fc_{22}) kann die globalen Auswirkungen aller seiner Komponenten in der Detaillierung verursachen.

Schritt 4.1: Sicherheitsstufen einem Fehlverhalten von Komponenten zuordnen

Der Maximalwert der Sicherheitsstufe der globalen Auswirkungen, der in einer Zeile einem Fehlverhalten zugeordnet ist wird in das entsprechende Element der Spalte SL eingetragen. Die Vorgehensweise ist in Figur 8d verdeutlicht.

Schritt 5: Maßnahmen zur Fehlererkennung und/oder Beherrschung

Die folgenden beiden Tabellen enthalten Maßnahmen zur Fehlererkennung und Beherrschung für Komponenten (Tabelle 2) und Kommunikationsbeziehungen (Tabelle 3).

Tabelle 2: Zusammenstellung von Maßnahmen zur Fehlererkennung und Beherrschung für funktionale Komponenten.

Fehlerart (Ursache)	Maßnahmen	
	Fehlererkennung	**Fehlerbeherrschung**
Komponente tot	• Bestätigung bzgl. Kommunikationsinhalt • Funktionsredundanz • Kontrollrechnung mit alternativen Eingangsgrößen • Kontrollrechnung/Abfrage mit Referenzwerten oder Eingangsmustern • Überwachung phys. und/oder elektr. Größen bei bekannten Randbedingungen • Zeitliche und logische Ablaufüberwachung	• Redundanz • Abschaltung der fehlerbeeinflussten Teilfunktion • Abschaltung der Elektronik auf Fzg.-Grundfunktion • Sicherer Abschaltzustand • System bleibt fehlerhaft in Betrieb • Fehler beseitigen • Situationsabhängige Strategieänderung zur Zielerreichung mit reduzierten Mitteln • Zusätzliche Mittel
Berechnet falsche Werte	• Bestätigung bzgl. Kommunikationsinhalt • Funktionsredundanz • Kontrollrechnung mit alternativen Eingangsgrößen • Kontrollrechnung/Abfrage mit Referenzwerten oder Eingangsmustern • Überwachung phys. und/oder elektr. Größen bei bekannten Randbedingungen	• Redundanz • Abschaltung der fehlerbeeinflussten Teilfunktion • Abschaltung der Elektronik auf Fzg.-Grundfunktion • Sicherer Abschaltzustand • System bleibt fehlerhaft in Betrieb • Fehler beseitigen • Situationsabhängige Strategieänderung zur Zielerreichung mit reduzierten Mitteln • Zusätzliche Mittel
Unkontrolliert aktiv	• Bestätigung bzgl. Kommunikationsinhalt • Funktionsredundanz • Kontrollrechnung mit alternativen Eingangsgrößen • Kontrollrechnung/Abfrage mit Referenzwerten oder Eingangsmustern • Überwachung phys. und/oder elektr. Größen bei bekannten Randbedingungen	• Redundanz • Abschaltung der fehlerbeeinflussten Teilfunktion • Abschaltung der Elektronik auf Fzg.-Grundfunktion • Sicherer Abschaltzustand • System bleibt fehlerhaft in Betrieb • Fehler beseitigen • Situationsabhängige Strategieänderung zur Zielerreichung mit reduzierten Mitteln • Zusätzliche Mittel

Tabelle 3: Zusammenstellung von Maßnahmen zur Fehlererkennung und Beherrschung für Kommunikationsbeziehungen

Fehlerart (Ursache)	Maßnahmen	
	Fehlererkennung	Fehlerbeherrschung
Unkontrolliert aktiv	• Bestätigung bzgl. Kommunikationsinhalt • Funktionsredundanz • Kontrollrechnung mit alternativen Eingangsgrößen • Kontrollrechnung/Abfrage mit Referenzwerten oder Eingangsmustern • Überwachung der Übertragungswege • Überwachung phys. und/oder elektr. Größen bei bekannten Randbedingungen • Zeitliche und logische Ablaufüberwachung • Dynamische Formulierung von Kommunikationen und errechneten Werten	• Redundanz • Abschaltung der fehlerbeeinflussten Teilfunktion • Abschaltung der Elektronik auf Fzg.-Grundfunktion • Sicherer Abschaltzustand • System bleibt fehlerhaft in Betrieb • Fehler beseitigen • Situationsabhängige Strategieänderung zur Zielerreichung mit reduzierten Mitteln • Zusätzliche Mittel • Zeit- und Logiksteuerungsüberwachung
Fehlleitung	• Bestätigung bzgl. Kommunikationsinhalt • Funktionsredundanz • Kontrollrechnung mit alternativen Eingangsgrößen • Kontrollrechnung/Abfrage mit Referenzwerten oder Eingangsmustern • Überwachung der Übertragungswege • Überwachung phys. und/oder elektr. Größen bei bekannten Randbedingungen • Zeitliche und logische Ablaufüberwachung • Dynamische Formulierung von Kommunikationen und errechneten Werten	• Redundanz • Abschaltung der fehlerbeeinflussten Teilfunktion • Abschaltung der Elektronik auf Fzg.-Grundfunktion • Sicherer Abschaltzustand • System bleibt fehlerhaft in Betrieb • Fehler beseitigen • Situationsabhängige Strategieänderung zur Zielerreichung mit reduzierten Mitteln • Zusätzliche Mittel

Unterbrechung	• Bestätigung bzgl. Kommunikationsinhalt • Funktionsredundanz • Kontrollrechnung mit alternativen Eingangsgrößen • Kontrollrechnung/Abfrage mit Referenzwerten oder Eingangsmustern • Überwachung phys. und/oder elektr. Größen bei bekannten Randbedingungen • Zeitliche und logische Ablaufüberwachung	• Redundanz • Abschaltung der fehlerbeeinflussten Teilfunktion • Abschaltung der Elektronik auf Fzg.-Grundfunktion • Sicherer Abschaltzustand • System bleibt fehlerhaft in Betrieb • Fehler beseitigen • Situationsabhängige Strategieänderung zur Zielerreichung mit reduzierten Mitteln • Zusätzliche Mittel
Information zur falschen Zeit	• Bestätigung bzgl. Kommunikationsinhalt • Funktionsredundanz • Kontrollrechnung mit alternativen Eingangsgrößen • Kontrollrechnung/Abfrage mit Referenzwerten oder Eingangsmustern • Überwachung phys. und/oder elektr. Größen bei bekannten Randbedingungen • Zeitliche und logische Ablaufüberwachung	• Redundanz • Abschaltung der fehlerbeeinflussten Teilfunktion • Abschaltung der Elektronik auf Fzg.-Grundfunktion • Sicherer Abschaltzustand • System bleibt fehlerhaft in Betrieb • Situationsabhängige Strategieänderung zur Zielerreichung mit reduzierten Mitteln • Zusätzliche Mittel
Ergebnis zur falschen Zeit	• Bestätigung bzgl. Kommunikationsinhalt • Funktionsredundanz • Kontrollrechnung mit alternativen Eingangsgrößen • Überwachung phys. und/oder elektr. Größen bei bekannten Randbedingungen • Zeitliche und logische Ablaufüberwachung	• Redundanz • Abschaltung der fehlerbeeinflussten Teilfunktion • Abschaltung der Elektronik auf Fzg.-Grundfunktion • Sicherer Abschaltzustand • System bleibt fehlerhaft in Betrieb • Fehler beseitigen • Situationsabhängige Strategieänderung zur Zielerreichung mit reduzierten Mitteln • Zusätzliche Mittel
Liefert falsche Information	• Bestätigung bzgl. Kommunikationsinhalt • Funktionsredundanz • Kontrollrechnung mit alternativen Eingangsgrößen • Kontrollrechnung/Abfrage mit Referenzwerten oder Eingangsmustern • Überwachung der Übertragungswege • Überwachung phys. und/oder elektr. Größen bei bekannten Randbedingungen	• Redundanz • Abschaltung der fehlerbeeinflussten Teilfunktion • Abschaltung der Elektronik auf Fzg.-Grundfunktion • Sicherer Abschaltzustand • System bleibt fehlerhaft in Betrieb • Fehler beseitigen • Situationsabhängige Strategieänderung zur Zielerreichung mit reduzierten Mitteln • Zusätzliche Mittel

Maßnahmen zur Fehlererkennung und/oder Fehlerbeherrschung auf einer hohen Abstraktionsebene anzugeben gestaltet sich schwierig, falls noch keine konkrete Systemrealisierung vorhanden ist. Für viele abstrakte Fehler in der CSA-Tabelle lassen sich nur dann wirksame und wirtschaftlich sinnvolle Maßnahmen zur Fehlererkennung und -beherrschung angeben, wenn diese realisierungsabhängig angegeben werden, d.h. für eine konkrete Systemtopologie. Bei realisierungsunabhängiger Betrachtung gibt es ansonsten zu viele Möglichkeiten, die auf abstrakter Ebene zur Lösung angegeben werden können (vgl. Tabelle 2 und Tabelle 3). Die Maßnahmen geben Möglichkeiten zur Erkennung und Beherrschung der abstrakten Ursachen an. Diese abstrakten Ursachen können als Fehler-Modi (Fehlerarten) der allgemeineren FS-Fehler verstanden werden (vgl. Definition 3).

Auf hoher Abstraktionsebene lassen sich Maßnahmen angeben, die schon in einer frühen Entwicklungsphase offensichtlich sind.

Dazu zählen Maßnahmen, welche die Fehlerausbreitung verhindern oder auf Plausibilität basieren. So kann offensichtlich sein, dass ein Signal nur innerhalb bestimmter Grenzwerte liegen darf. Fehlerausbreitung kann durch Redundanz eingegrenzt werden. Redundante Strukturen können in späteren Entwicklungsphasen, d.h. bei detaillierter Kenntnis der realisierten Topologie in kostengünstige Maßnahmen umgewandelt werden. Ein Beispiel hierfür sind Codes zur Fehlererkennung und -korrektur. Die klartextlichen Angaben der Tabellen sind im Programm bzw. Computersystem durch Kodierungen verkürzbar und zuordenbar.

Eine optimale Lösung technischer und wirtschaftlicher Art kann erst dann gefunden werden, wenn man einen Fehler innerhalb einer bekannten Topologie betrachtet. Wird für eine Abfrage die Ursache *„liefert falsche Information"* als kritisch identifiziert, so hängt die zu treffende Maßnahme sehr stark davon ab, wie die Abfrage realisiert ist. Wird der Wert innerhalb eines Prozessorsystems abgefragt (z.B. interner Speicher), so ist evtl. keine Maßnahme zu treffen (eigensicher) bzw. man kann das Prozessorsystem als gesamte Einheit betrachten

und somit eine Vielzahl von Operationen mit einer einzigen Maßnahme überwachen, z.B. Watchdog-Timer. Läuft die Kommunikation über eine externe Verbindung (Kabel, Bussystem), so muss die Verbindung/Nachrichtenübertragung eventuell redundant ausgelegt werden. Bei EMV Problemen genügt es ggf. schon, wenn man eine Verbindung über ein geschirmtes Kabel ohne jeglichen zusätzlichen elektronischen Aufwand gewährleisten kann.

Schritt 6: CARTRONIC® - Sicherheitsstruktur

Die CARTRONIC®-Darstellung eines Systems (dargestellt für ein Beispiel in Figur 2) kann abgebildet werden in ein CARTRONIC®-UML Modell (Figur 3). Dies erlaubt eine formalere Systemspezifikation als CARTRONIC®. Außerdem ist UML eine international genormte Sprache. Für die Beschreibung einer Systemtopologie ist es jedoch erforderlich das bestehende CARTRONIC®-UML Modell zu erweitern. Die Erweiterung muss die Abbildung der Maßnahmen zur Fehlererkennung und -beherrschung, die Partitionierung der Funktionen auf Steuergeräte und die Darstellung von zeitlichen und logischen Abläufen umfassen. Die erweiterte Struktur kann zur Dokumentation der verwendeten Sicherheitsmaßnahmen verwendet werden. Eine Darstellung, in welcher Struktur, Funktionalität und Topologie enthalten sind, ist auch geeignet für zukünftige quantitative Systemanalysen, insbesondere zur automatisierten Durchführung.

Schritt 7: Verifikation

Bei der Verifikation wird überprüft, ob die Resultate der CARTRONIC® basierten Sicherheitsanalyse dazu führen, dass eine Produktspezifikation erfüllt wird. Es wird untersucht, ob die vergebenen Sicherheitsstufen den Anforderungen der Spezifikation entsprechen, ob also die zu erzielenden Sicherheitsstufen mit vorgebbaren und somit zu erzielenden übereinstimmen. Ist dies

nicht der Fall, so kann eine weitere Iteration der CARTRONIC® basierten Sicherheitsanalyse durchlaufen werden. Dieser iterative Verbesserungsprozess wird so lange fortgeführt, bis alle Anforderung der Spezifikation bzw. der vorgegeben Sicherheitsstufen erfüllt sind.

In Figur 12 ist die Einordnung der CSA in einen Entwicklungsprozess dargestellt. Der verwendete Entwicklungsprozess orientiert sich am V-Modell. Das V-Modell ist ein Entwicklungsstandard des Bundes für IT-Systeme. Es ist möglich das V-Modell projektspezifisch an gegebene Randbedingungen anzupassen. Dieser Vorgang wird als *Tailoring* bezeichnet. Im V-Modell werden Tätigkeiten (Aktivitäten) und ihre Produkte festgelegt. Das für den CARTRONIC® basierten Entwicklungsprozess angepasste inkrementelle, iterative V-Modell (IIV-Modell) wird auf den drei Ebenen Systemebene, Subsystemebene und Teilrealisierungsebene angewendet. Die Navigation im IIV-Modell erfolgt entlang der eingezeichneten Pfeile. Es ist möglich von der linken auf die rechte Seite einer Ebene des V-Modells (Testfälle) und zurück (Iterationen) zu gelangen. Zwischen den Ebenen sind auch mehrere Inkremente möglich. Auf der Teilrealisierungsebene kann beispielsweise erkannt werden, dass zusätzliche Funktionen für eine Realisierung benötigt werden. Es kann dann ein zusätzliches Inkrement durchlaufen werden indem auf der Subsystemebene die Funktionen und ihre Interaktionen eingeführt werden und diese dann ihrerseits auf der Teilrealisierungsebene realisiert werden. Auf der Systemebene wird das Kraftfahrzeug als Ganzes betrachtet. Die Subsystemebene detailliert das Gesamtsystem Kraftfahrzeug in Teilsysteme. Diese Teilsysteme können beispielsweise die Motorsteuerung, das Bremssystem, das Getriebe oder ein Adaptive Cruise Control sein. Die Subsystemebene stellt die Teilsysteme des Kraftfahrzeugs noch realisierungsunabhängig dar, d.h. es wird lediglich die Funktionalität nicht jedoch die technische Realisierung betrachtet. Auf der Teilrealisierungsebene wird jedes Subsystem weiter detailliert.

Es wird eine Entscheidung über eine Topologie getroffen und ob eine Funktion als Software, Computer Hardware, Hydraulik, Elektronik, Elektrik, Mechanik etc. realisiert wird. Anschließend wird ein entsprechendes Subsystem erstellt und gegebenenfalls die Software implementiert. Auf jeder Ebene des IIV-Modells wird auf der linken Seite des V-Modells eine Anforderungsanalyse durchgeführt und ein Entwurf angefertigt. Die rechte Seite des IIV-Modells dient der Integration und der Verifikation des auf der entsprechenden Ebene erstellten Entwurfs. Auf der Systemebene kann zusätzlich zu den beschriebenen Vorgängen eine Validation durchgeführt werden. Eine Validation prüft, ob die Systemspezifikation die an sie gestellten Anforderungen erfüllt. Die Verifikation hingegen überprüft ein Produkt gegenüber der Spezifikation.

Die Vorgehensschritte Schritt 1 bis Schritt 5 werden in der Analysephase der Subsystemebene durchgeführt. Schritt 6 wird in der Entwurfsphase der Subsystemebene umgesetzt. Aufgrund der Überlegungen in Schritt 5, nämlich dass eine Konkretisierung von Maßnahmen zur Fehlererkennung und Beherrschung häufig erst bei bekannter Systemtopologie sinnvoll ist, empfiehlt sich eine Detaillierung der Sicherheitsmaßnahmen in Schritt 5 und Schritt 6 auf der Teilrealisierungsebene durchzuführen. In dieser Phase wird die Systemtopologie, d.h. die Partitionierung der Funktionalitäten auf Steuergeräte vorgenommen und die Funktionsrealisierungen festgelegt. Die CSA, wie sie hier beschrieben ist, wird also hauptsächlich auf der Subsystemebene angewendet. Es ist jedoch vorteilhaft die CSA auch auf der Teilrealisierungsebene fortzuführen. Hier wird eine Anforderungsanalyse durchgeführt, wie Sicherheitsmaßnahmen in Abhängigkeit der Topologie und der Realisierung des Teilsystems zu gestalten sind und ein entsprechender Entwurf angefertigt. Dieser Entwurf und seine Integration können auf der rechten Seite des IIV-Modells verifiziert werden.

Die gezeigte Erfindung kann automatisiert auf einem Computersystem ablaufen. Dazu sind die einzelnen Schritte oder Teile dieser Schritte ebenso wie die Tabellen als Computerprogramm mit Daten und Befehlen darstellbar, so dass die Schritte 1 bis 7 als Programmcode abgespeichert werden können und in einer Einrichtung insbesondere einem Computersystem zur Ausführung gelangen um ein erfindungsgemäßes Verfahren auszuführen. Als Speicher bzw. Datenträger kann hierbei jede denkbare Form gelten wie z.B. CD-ROM, DVD, Diskette, EPROM, FlashEPROM, ROM, RAM, usw. wodurch ein Computerprogrammprodukt in Verbindung mit dem Computerprogramm vorliegt. Insbesondere eine Übertragung des Programms via Netzwerken wie Internet von einem Speicher zu einem anderen Speicher bzw. Netzwerkteilnehmer fällt ebenfalls darunter.

Ansprüche

1. Verfahren zur Durchführung einer Sicherheitsanalyse bei Systemen, insbesondere in einem Kraftfahrzeug, wobei die Systeme oder das wenigstens eine System aus mehreren Komponenten bestehen, zwischen denen Kommunikationsbeziehungen bestehen, wobei die Komponenten und deren Kommunikationsbeziehungen eine Funktionsstruktur der Systeme oder des wenigstens einen Systems bilden, dadurch gekennzeichnet, dass Fehler in Abhängigkeit von der Funktionsstruktur ermittelt werden und diese Fehlerabhängigkeiten bezüglich der Funktionsstruktur ausgewertet werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Fehlerabhängigkeiten in der Funktionsstruktur nachverfolgt werden, wodurch Fehlerpfade generiert werden, wobei globale Auswirkungen der Fehler als Abschluß der Fehlerpfade ermittelt werden.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Fehlerabhängigkeiten in der Funktionsstruktur nachverfolgt werden, wodurch Fehlerpfade generiert werden, wobei globale Auswirkungen der Fehler als Abschluß der Fehlerpfade ermittelt und bewertet werden.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass die globalen Auswirkungen durch Ermittlung wenigstens einer Sicherheitsstufe bewertet werden.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass zusätzlich zu den Fehlerabhängigkeiten bezüglich der Funktionsstruktur Fehler ermittelt werden, welche ein Fehlverhalten einer Komponente oder einer Kommunikationsbeziehung bewirken.

6. Verfahren nach Anspruch 2 oder 3 und 5, dadurch gekennzeichnet, dass Fehlverhalten einer Komponente oder einer Kommunikationsbeziehung zu den globalen Auswirkungen zugeordnet werden.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass Maßnahmen zur Fehlererkennung und/oder Fehlerbeherrschung ermittelt werden.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Funktionsstruktur dahingehend erweitert wird, dass die globalen Auswirkungen und/oder dass Fehlverhalten einer Komponente oder einer Kommunikationsbeziehung berücksichtigt wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Funktionsstruktur dahingehend erweitert wird, dass Maßnahmen zur Fehlererkennung und/oder Fehlerbeherrschung einbezogen werden.

10. Verfahren zur Erzielung einer vorgebbaren Sicherheitsstufe bei Systemen, insbesondere in einem Kraftfahrzeug, wobei die Systeme oder wenigstens ein System aus mehreren Komponenten bestehen, zwischen denen Kommunikationsbeziehungen bestehen,

wobei die Komponenten und deren Kommunikationsbeziehungen eine Funktionsstruktur der Systeme bilden, wobei Fehler in Abhängigkeit von der Funktionsstruktur ermittelt werden und diese Fehlerabhängigkeiten bezüglich der Funktionsstruktur ausgewertet werden mit folgenden Schritten:

a) Verfolgung der Fehlerabhängigkeiten in der Funktionsstruktur und Generation von Fehlerpfaden sowie Ermittlung von globalen Auswirkungen der Fehler,
b) Bewertung der globalen Auswirkungen in Abhängigkeit vorgebbarer Sicherheitsstufen,
c) Ermittlung von Fehlern, welche ein Fehlverhalten einer Komponente oder einer Kommunikationsbeziehung bewirken,
d) Zuordnung des Fehlverhaltens einer Komponente oder einer Kommunikationsbeziehung zu den globalen Auswirkungen
e) Ermittlung von Maßnahmen zur Fehlererkennung und/oder Fehlerbeherrschung,
f) Ermittlung der erzielbaren Sicherheitsstufe und Vergleich der ermittelten Sicherheitsstufe mit der zu erzielenden Sicherheitsstufe und
g) in Abhängigkeit von dem Vergleich erneuter Verfahrensstart bei a), bis die zu erzielende Sicherheitsstufe erzielt ist.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass zwischen den Schritten e) und f) eine Dokumentation der Funktionsstruktur erfolgt.

12. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Funktionsstruktur als CARTRONIC®-Funktionsstruktur unter Verwendung der UML dargestellt wird.

13. Einrichtung, insbesondere Computersystem, zur Durchführung eines Verfahrens gemäß wenigstens einem der Ansprüche 1 bis 12.

14. Computerprogramm, welches bei Ablauf in einer Einrichtung nach Anspruch 13 ein Verfahren gemäß wenigstens einem der Ansprüche 1 bis 12 ausführt.

15. Computerprogrammprodukt, insbesondere ein Datenträger mit einem Computerprogramm nach Anspruch 14, welches bei Einbringung in eine Einrichtung nach Anspruch 13 ein Verfahren nach wenigstens einem der Ansprüche 1 bis 12 ausführt.

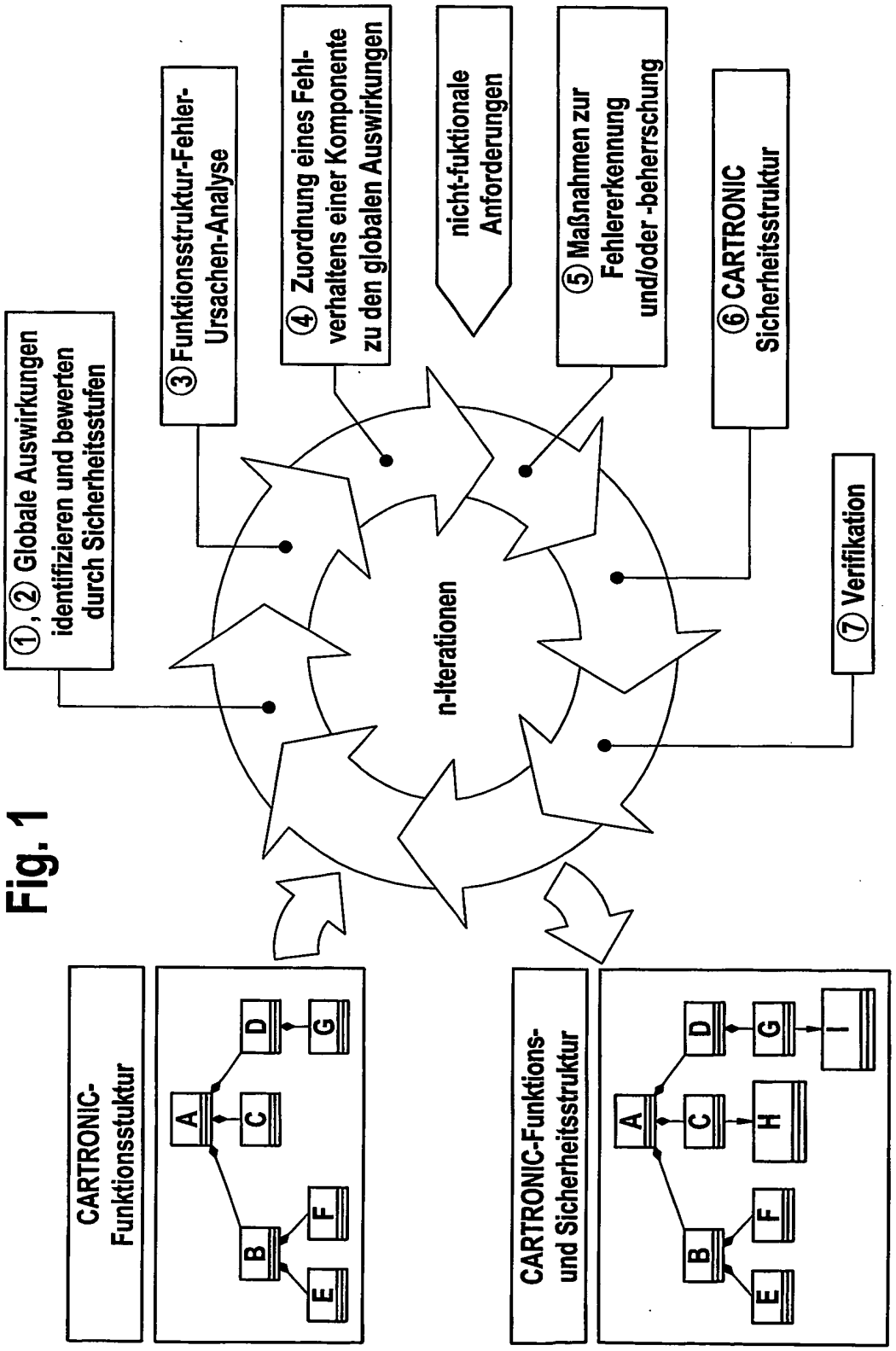

①, ② Globale Auswirkungen identifizieren und bewerten durch Sicherheitsstufen
③ Funktionsstruktur-Fehler-Ursachen-Analyse
④ Zuordnung eines Fehlverhaltens einer Komponente zu den globalen Auswirkungen
nicht-fuktionale Anforderungen
⑤ Maßnahmen zur Fehlererkennung und/oder -beherrschung
⑥ CARTRONIC Sicherheitsstruktur
⑦ Verifikation
n-Iterationen
CARTRONIC-Funktionsstuktur
A
B
C
D
E
F
G
CARTRONIC-Funktions- und Sicherheitsstruktur
A
B
C
D
E
F
G
H
I

Fig. 1

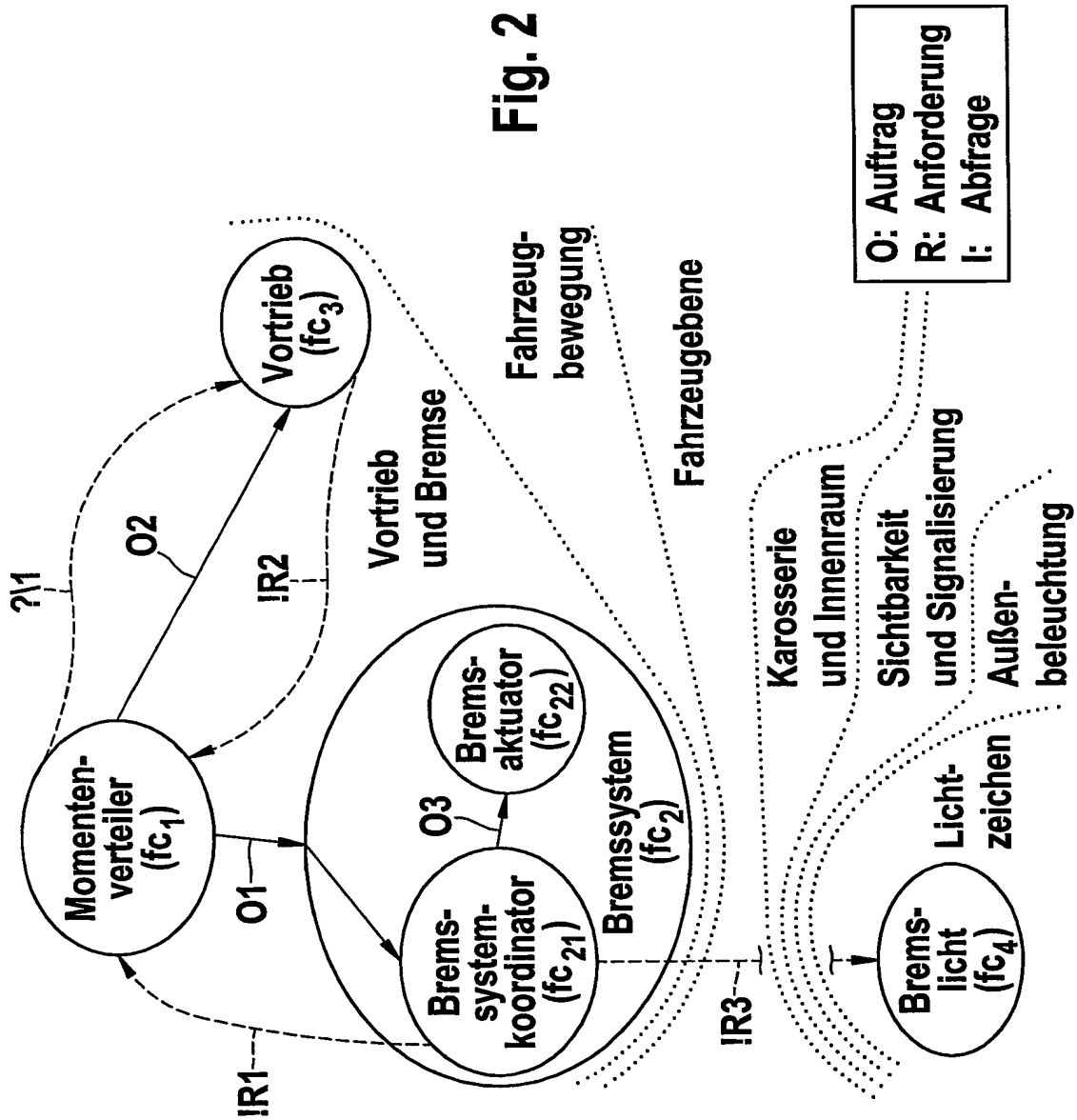

Momenten-verteiler (fc_1)
Vortrieb (fc_3)
Brems-system-koordinator (fc_{21})
Brems-aktuator (fc_{22})
Bremssystem (fc_2)
Brems-licht (fc_4)
Licht-zeichen
?!1
O1
O2
O3
!R1
!R2
!R3
Vortrieb und Bremse
Fahrzeug-bewegung
Fahrzeugebene
Karosserie und Innenraum
Sichtbarkeit und Signalisierung
Außen-beleuchtung
O: Auftrag
R: Anforderung
I: Abfrage

Fig. 2

Fig. 3

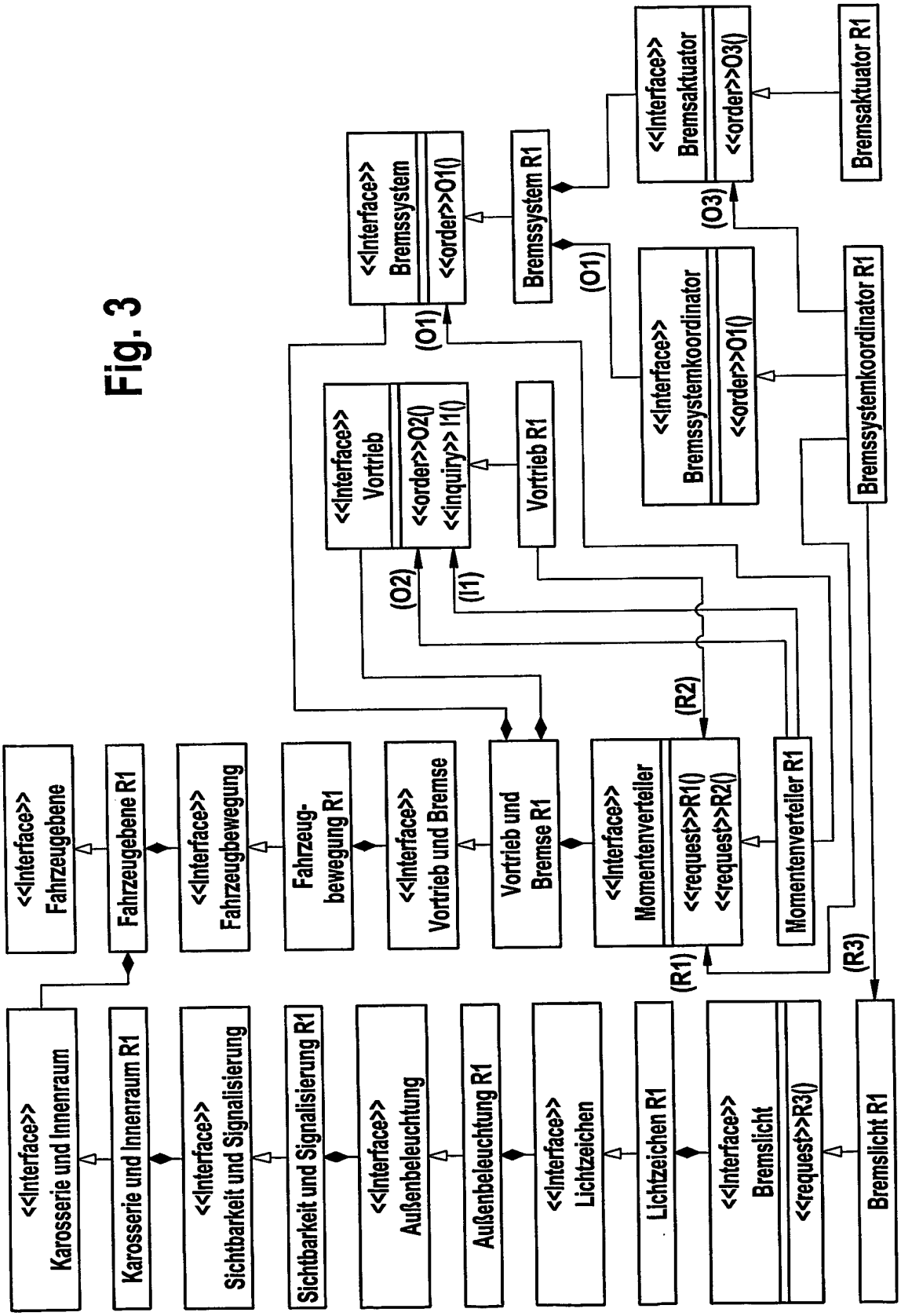
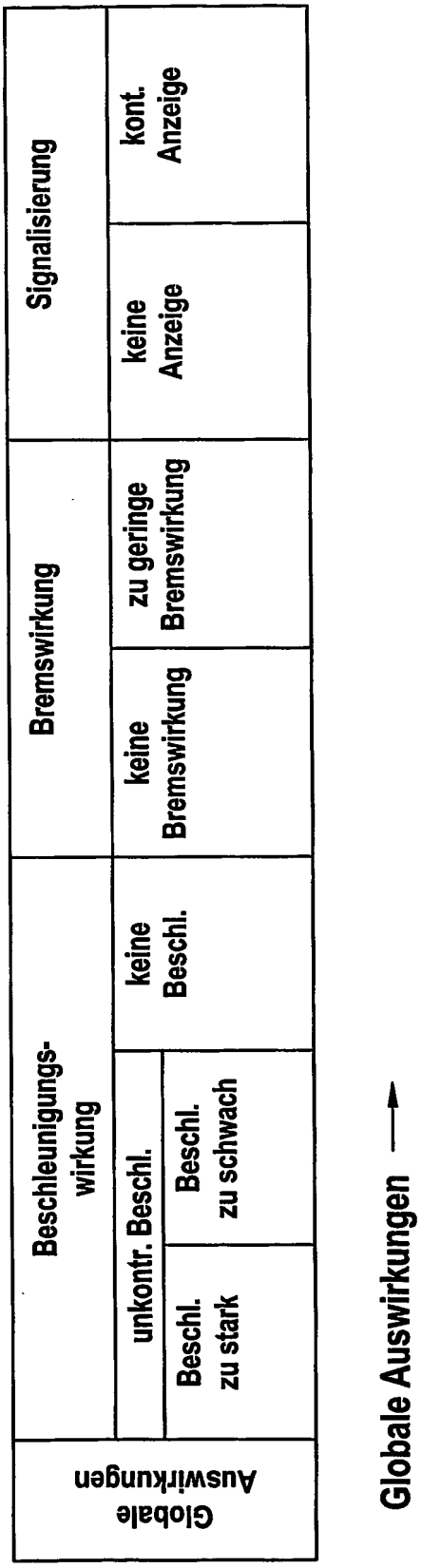

<<Interface>> Karosserie und Innenraum
Karosserie und Innenraum R1
<<Interface>> Sichtbarkeit und Signalisierung
Sichtbarkeit und Signalisierung R1
<<Interface>> Außenbeleuchtung
Außenbeleuchtung R1
<<Interface>> Lichtzeichen
Lichtzeichen R1
<<Interface>> Bremslicht
<<request>>R3()
Bremslicht R1
<<Interface>> Fahrzeugebene
Fahrzeugebene R1
<<Interface>> Fahrzeugbewegung
Fahrzeug-bewegung R1
<<Interface>> Vortrieb und Bremse
Vortrieb und Bremse R1
<<Interface>> Momentenverteiler
<<request>>R1()
<<request>>R2()
Momentenverteiler R1
<<Interface>> Vortrieb
<<order>>O2()
<<inquiry>> I1()
Vortrieb R1
<<Interface>> Bremssystem
<<order>>O1()
Bremssystem R1
<<Interface>> Bremssystemkoordinator
<<order>>O1()
Bremssystemkoordinator R1
<<Interface>> Bremsaktuator
<<order>>O3()
Bremsaktuator R1
(O1)
(O2)
(I1)
(R1)
(R2)
(R3)
(O1)
(O3)

Fig. 4


Globale Auswirkungen
Globale Auswirkungen
Beschleunigungs-wirkung
unkontr. Beschl.
Beschl. zu stark
Beschl. zu schwach
keine Beschl.
Bremswirkung
keine Bremswirkung
zu geringe Bremswirkung
Signalisierung
keine Anzeige
kont. Anzeige

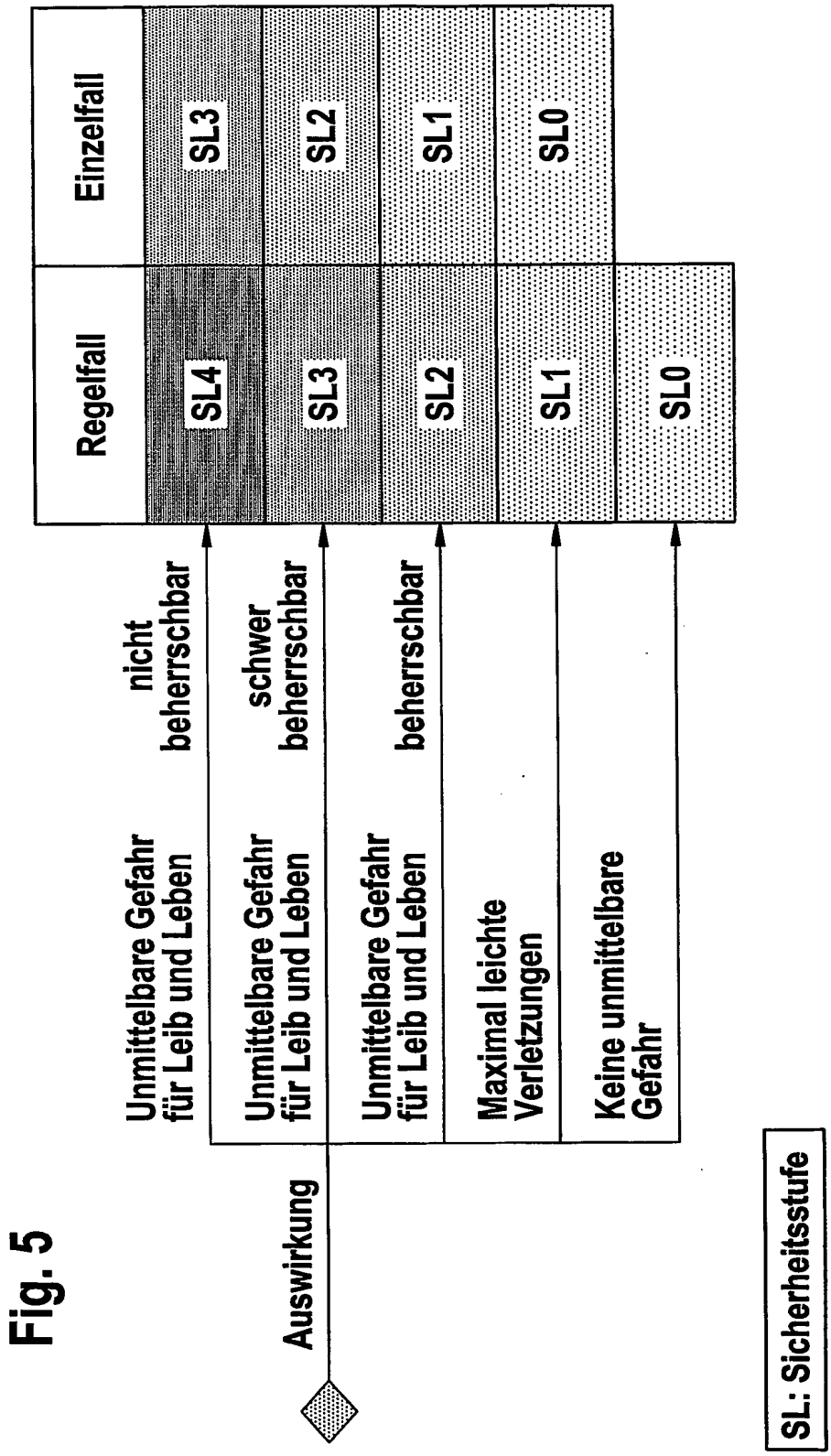

Einzelfall
Regelfall
SL3
SL2
SL1
SL0
SL4
SL3
SL2
SL1
SL0
Auswirkung
Unmittelbare Gefahr für Leib und Leben
nicht beherrschbar
Unmittelbare Gefahr für Leib und Leben
schwer beherrschbar
Unmittelbare Gefahr für Leib und Leben
beherrschbar
Maximal leichte Verletzungen
Keine unmittelbare Gefahr
SL: Sicherheitsstufe

Fig. 5

Fig. 6

Globale Auswirkungen			Beschleunigungswirkung			Bremswirkung		Signalisierung	
			unkontr. Beschl.		keine Beschl.	keine Bremswirkung	zu geringe Bremswirkung	keine Anzeige	kont. Anzeige
SL			Beschl. zu stark	Beschl. zu schwach					
			3	1	1	4	3	1	1

Globale Auswirkungen	Beschleunigungswirkung		Bremswirkung		Signalisierung		Fehlverhalten Komponenten / Funktionsstruktur	fc_1		fc_2		fc_{21}		fc_{22}		fc_3		fc_4	
	unkontr. Beschl.	keine Beschl.	keine Bremsw.	zu geringe Bremsw.	keine Anzeige	Kont. Anzeige		C	M	C	M	C	M	C	M	C	M	C	M
SL	2	1	4	3	1	1													
							fc_1	x	R_R1 R_R2 I_I1										
							fc_2			x	O_O1								
							fc_{21}					x	O_O1						
							fc_{22}							x	O_O3				
							fc_3									x	O_O2		
							fc_4											x	R_R3

Fig. 7

Für die Komponenten werden die folgenden Abkürzungen verwendet:

fc_1 → Momentenverteiler
fc_2 → Bremssystem
fc_{21} → Bremssystemkoordinator
fc_{22} → Bremsaktuator
fc_3 → Vortrieb
fc_4 → Bremslicht

Die Spalten C und M in der Funktionsstruktur stehen für:

C: Komponente (component)
M: Kommunikation (message)

Globale Auswirkungen	Beschleunigungs-wirkung		Bremswirkung		Signalisierung		Fehlverhalten Komponenten Funktionsstruktur	fc_1		fc_2						fc_3		fc_4	
	unkontr. Beschl.	keine Beschl.	keine Bremsw.	zu geringe Bremsw.	keine Anzeige	Kont. Anzeige						fc_{21}		fc_{22}					
SL	2	1	4	3	1	1		C	M	C	M	C	M	C	M	C	M	C	M
							fc_1	x	R_R1 R_R2 I_I1			x	O_O1			x	O_O2		
							fc_2	x	R_R1 R_R2 I_I1	x	O_O1					x	O_O2		
							fc_{21}	x	R_R1 R_R2 I_I1			x	O_O1			x	O_O2		
							fc_{22}	x	R_R1 R_R2 I_I1			x	O_O1	x	O_O3 R_R1	x	O_O2		
							fc_3	x	R_R1 R_R2 I_I1			x	O_O1			x	O_O2		
							fc_4	x	R_R1 R_R2 I_I1			x	O_O1			x	O_O2	x	R_R3

Fig. 8a

Für die Komponenten werden die folgenden Abkürzungen verwendet:

fc_1 → Momentenverteiler
fc_2 → Bremssystem
fc_{21} → Bremssystemkoordinator
fc_{22} → Bremsaktuator
fc_3 → Vortrieb
fc_4 → Bremslicht

Die Spalten C und M in der Funktionsstruktur stehen für:

C: Komponente (component)
M: Kommunikation (message)

ERSATZBLATT (REGEL 26)

Globale Auswirkungen								Fehlverhalten Komponenten Funktionsstruktur	fc_1			fc_2						fc_3			fc_4		
	Beschleunigungswirkung		Bremswirkung			Signalisierung									fc_{21}			fc_{22}					
SL	unkontr. Beschl.	keine Beschl.	keine Bremsw.	zu geringe Bremsw.	keine Anzeige	Kont. Anzeige			C	M		C	M		C	M		C	M		C	M	
	2	1	4	3	1	1																	
							fc_1		x	R_R1 R_R2 I_I1					x	O_O1			x	O_O2			
							fc_2		x	R_R1 R_R2 I_I1		x	O_O1						x	O_O2			
								fc_{21}	x	R_R1 R_R2 I_I1					x	O_O1			x	O_O2			
								fc_{22}	x	R_R1 R_R2 I_I1					x	O_O1	x	O_O3 R_R1	x	O_O2			
							fc_3		x	R_R1 R_R2 I_I1					x	O_O1			x	O_O2			
							fc_4		x	R_R1 R_R2 I_I1					x	O_O1			x	O_O2	x	R_R3	

Für die Komponenten werden die folgenden Abkürzungen verwendet:

fc_1 → Momentenverteiler
fc_2 → Bremssystem
fc_{21} → Bremssystemkoordinator
fc_{22} → Bremsaktuator
fc_3 → Vortrieb
fc_4 → Bremslicht

Die Spalten C und M in der Funktionsstruktur stehen für:

C: Komponente (component)
M: Kommunikation (message)

Fig. 8b

Globale Auswirkungen	Beschleunigungswirkung		Bremswirkung		Signalisierung		Fehlverhalten Komponenten	Funktionsstruktur	fc_1		fc_2				fc_3		fc_4	
	unkontr. Beschl.	keine Beschl.	keine Bremsw.	zu geringe Bremsw.	keine Anzeige	Kont. Anzeige							fc_{21}		fc_{22}			
SL	2	1	4	3	1	1			C	M	C	M	C	M	C	M	C	M
	x	x	x	x	x	x	fc_1		x	R_R1 R_R2 I_I1			x	O_O1			x	O_O2
	x	x	x	x	x	x	fc_2		x	R_R1 R_R2 I_I1	x	O_O1					x	O_O2
	x	x	x	x	x	x		fc_{21}	x	R_R1 R_R2 I_I1			x	O_O1			x	O_O2
			x	x				fc_{22}	x	R_R1 R_R2 I_I1			x	O_O1	x	O_O3 R_R1	x	O_O2
	x	x	x	x	x	x	fc_3		x	R_R1 R_R2 I_I1			x	O_O1			x	O_O2
					x	x	fc_4		x	R_R1 R_R2 I_I1			x	O_O1			x	O_O2	x	R_R3

Für die Komponenten werden die folgenden Abkürzungen verwendet:

fc_1 → Momentenverteiler
fc_2 → Bremssystem
fc_{21} → Bremssystemkoordinator
fc_{22} → Bremsaktuator
fc_3 → Vortrieb
fc_4 → Bremslicht

Fig. 8c

Die Spalten C und M in der Funktionsstruktur stehen für:

C: Komponente (component)
M: Kommunikation (message)

ERSATZBLATT (REGEL 26)

Globale Auswirkungen	Beschleunigungs-wirkung		Bremswirkung		Signalisierung		SL	Fehlverhalten Komponenten Funktionsstruktur	fc1		fc2		fc21		fc22		fc3		fc4	
	unkontr. Beschl.	keine Beschl.	keine Bremsw.	zu geringe Bremsw.	keine Anzeige	Kont. Anzeige														
SL	2	1	4	3	1	1			C	M	C	M	C	M	C	M	C	M	C	M
	x	x	x	x	x	x	4	fc1	x	R_R1 R_R2 I_I1			x	O_01			x	O_02		
	x	x	x	x	x	x	4	fc2	x	R_R1 R_R2 I_I1	x	O_01					x	O_02		
	x	x	x	x	x	x	4	fc21	x	R_R1 R_R2 I_I1			x	O_01			x	O_02		
			x	x			4	fc22	x	I R_R1 R_R2 I_I1			x	O_01	x	O_03	x	O_02		
	x	x	x	x	x	x	4	fc3	x	R_R1 R_R2 I_I1			x	O_01			x	O_02		
					x	x	1	fc4	x	R_R1 R_R2 I_I1			x	O_01			x	O_02	x	R_R3

Für die Komponenten werden die folgenden Abkürzungen verwendet:

fc_1 → Momentenverteiler
fc_2 → Bremssystem
fc_{21} → Bremssystemkoordinator
fc_{22} → Bremsaktuator
fc_3 → Vortrieb
fc_4 → Bremslicht

Fig. 8d

Die Spalten C und M in der Funktionsstruktur stehen für:

C: Komponente (component)
M: Kommunikation (message)

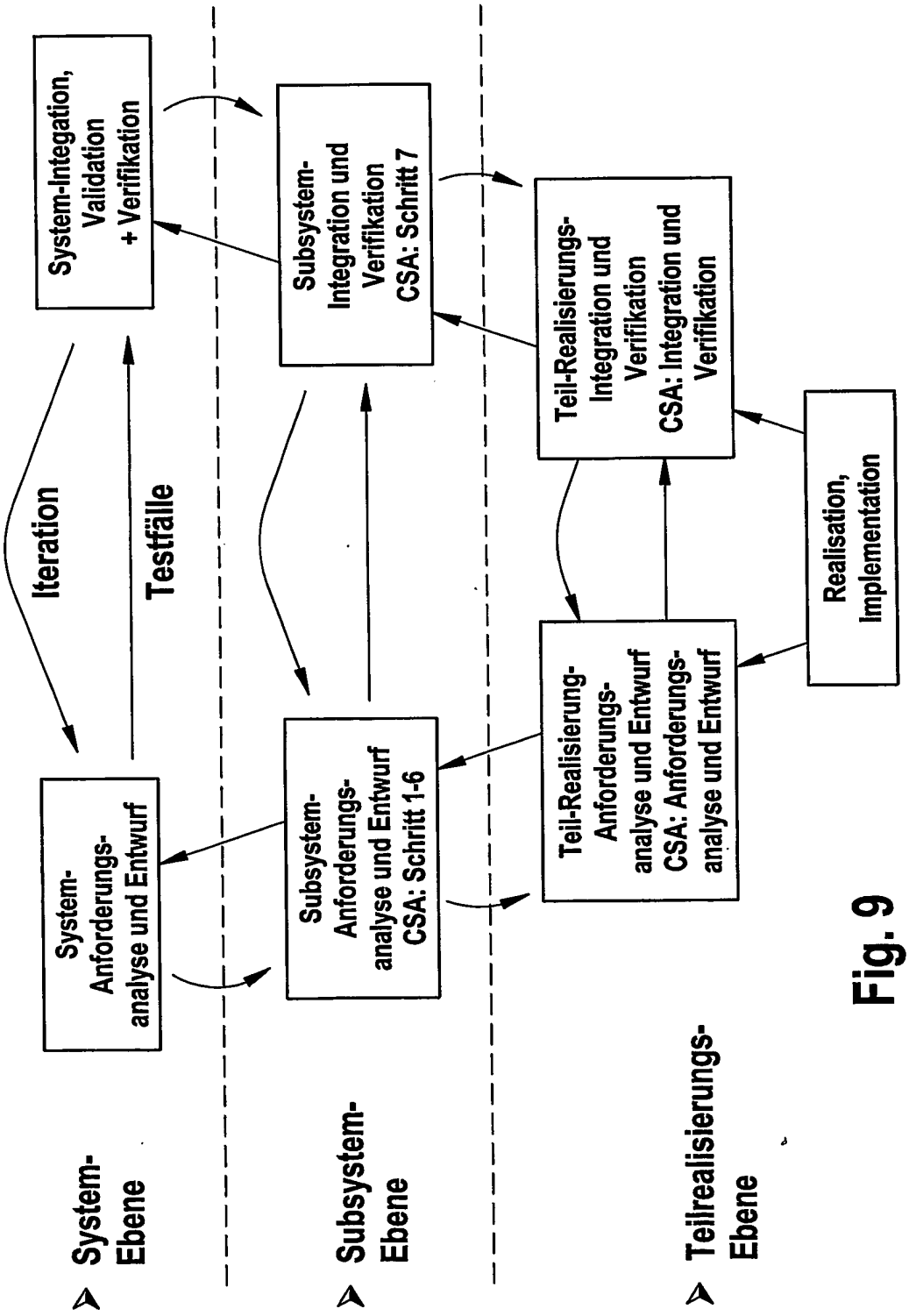

System-Integration, Validation + Verifikation
Subsystem-Integration und Verifikation CSA: Schritt 7
Teil-Realisierungs-Integration und Verifikation CSA: Integration und Verifikation
Iteration
Testfälle
System-Anforderungs-analyse und Entwurf
Subsystem-Anforderungs-analyse und Entwurf CSA: Schritt 1-6
Teil-Realisierung-Anforderungs-analyse und Entwurf CSA: Anforderungs-analyse und Entwurf
Realisation, Implementation
System-Ebene
Subsystem-Ebene
Teilrealisierungs-Ebene

Fig. 9